Blackmores

BS 10012 Case Study

Who are ONI

Established in 1992, ONI plc is a leading provider of IT solutions and services to both public sector and commercial markets. Privately owned, they offer a comprehensive range of on-site, cloud and hybrid technology solutions.

By adopting a strategic, forward-thinking approach to IT, they help clients drive revenue growth, reduce costs, improve productivity and, ultimately, enhance customer satisfaction and loyalty.

Why certification to BS 10012 is important to ONI

ONI recognise the importance of putting in place a framework for Personal Information Management, which allows them to maintain alignment to the requirements of data protection legislation (GDPR and forthcoming Data Protection Bill), and to also continually improve controls related to data protection and Information Asset security resulting in improved risk mitigation for the business.

The General Data Protection Regulation (GDPR) is a requirement that must be adopted by all businesses dealing with Personal Data by the 25th May 2018, or face fine up to 20 million euro OR 4% of the global turnover (whichever is greater).

Pioneering Standards BS10012 was updated in 2017 to align with the requirements of GDPR, and provides the framework for best practice in Personal Information Management. Formal certification to BS10012 is now offered by recognised certification bodies in the UK for the first time.

ONI took the pioneering decision to become one of the first organisations to seek formal certification to the revised BS10012 Standard, demonstrating that Personal Information Management is a top priority for ONI thus ensuring that both staff and client data is stored securely and fairly processed.

Approach taken

Having engaged Blackmores for their ISO 27001 certification in 2014, and through continued support for both ISO 9001(Quality) and ISO 27001 (Information Security), ONI once again engaged in the services of Blackmores for their BS 10012 journey in September 2017.

Recognising the importance of strong leadership commitment, the journey commenced with an initial awareness session with the senior team at ONI to convey the requirements of BS 10012 and what it means for ONI, their own personal data and the hosted services that they provide.

continued overleaf...

Embarking on the BS 10012 Journey

The approach to achieving BS 10012 is similar to the recognised approach to achieving GDPR compliance, but with a focus on recognising the needs and expectations of interested parties and taking a risk-based approach to data protection and control.

A top priority, and possibility the most fundamental requirement for successful compliance, is the need for strong leadership to secure commitment to demonstrating data protection best practice within the organisation. Within ONI, this was clearly demonstrated throughout the entire project, with Senior Management remaining as data champions beyond certification.

Thereafter, there is a requirement to understand Personal Information within the organisation which is achieved through mapping all data streams using a PIA (Privacy Impact Assessment). Once personal Information was understood for ONI and collated into a data inventory, it could then be risk assessed and the controls reviewed to ensure they provided the required level of risk mitigation. It was also vital to be able to understand the data flow for personal data within ONI.

As ONI is certified to ISO 9001:2015 and ISO 27001:2013 there were already robust policies and procedures in place already for both data protection and information security, however these were reviewed and updated as required for BS10012:2017.

It is well understood that people usually form the weakest link in terms of data protection or information security compliance. Therefore ONI recognised the importance of ensuring that all staff, at all levels were subject to BS10012 awareness training, incorporating elements relating to both data protection and information security. The final piece of the jigsaw puzzle to implement prior to certification was an element of internal compliance checking, achieved through both internal auditing and Management Review.

ISOQAR were selected as the preferred certification body for BS10012:2017 as they were the first certification body to be in a position to offer certification to the BS10012 Standard. A recommendation for certification was received from ISOQAR on the 6th February 2018, following a two stage audit conducted in December 2017 (Stage 1) and February 2018 (Stage 2).

This certification provides ONI with a clear competitive edge; one that demonstrates that management of personal data is a top priority within ONI. Being the first in achieving BS 10012

> *"Becoming accredited to BS10012 provides independent verification that ONI is an industry leader in data protection compliance, adding value and peace of mind to customers that our data procedures are robust and secure."*